AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently amended.) A method for establishing secure communication between a ~~first communicating~~ calling party and a ~~second communicating~~ called party, ~~comprising~~ consisting essentially of:

identifying a first shared random number associated with a ~~first communicating~~ calling party;

identifying a second shared random number associated with a ~~second communicating~~ called party;

identifying said calling party to said called party;

generating a public-private key pair by said called party;

transmitting a first message from said ~~second communicating~~ called party to said ~~first communicating~~ calling party, said first message including said first shared random number and said public portion of said public-private key pair, and said first message being encoded with a symmetric encryption key;

transmitting a second message from said ~~first communicating~~ calling party to said ~~second communicating~~ called party, said second message including said second shared random number, and said second message being encoded with ~~an asymmetric encryption key~~ said public portion of said public-private key pair; and

obtaining a shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number.

2. (Previously Presented.) The method of claim 1, wherein said combining function includes a logical function.

3. (Previously Presented.) The method of claim 2, wherein said logical function includes an exclusive or (XOR) function.

4. (Cancelled.)

5. (Previously Presented.) The method of claim 1, further comprising the step of transmitting a second message from said second computer to said first computer, said second message including said second shared random number.

6. (Previously Presented.) The method of claim 5, wherein said first message is encoded using an encoded password.

7. (Previously Presented.) The method of claim 6, wherein said encoded password is an encrypted password.

8. (Previously Presented.) The method of claim 6, wherein said step of encoding said first message comprises encrypting said first message using said encoded password.

9. (Previously Presented.) The method of claim 5, wherein said first message also includes an asymmetric key.

10.–153. (Cancelled.)